DOI: 10.1111/spc3.12507

ARTICLE

WILEY

The psychology of privacy in the digital age

Avelie Stuart[1] | Arosha K. Bandara[2] | Mark Levine[1,3]

[1]Department of Psychology, University of Exeter, Exeter, United Kingdom

[2]Computing and Communications, The Open University, Buckinghamshire, United Kingdom

[3]Department of Psychology, Lancaster University, Lancaster, United Kingdom

Correspondence
Avelie Stuart, Psychology, University of Exeter, Washington Singer Labs, Perry Road, Exeter, UK, EX4 4QG.
Email: a.stuart@exeter.ac.uk

Funding information
Engineering and Physical Sciences Research Council, Grant/Award Numbers: EP/K033433/1, EP/R013144/1

Abstract

Privacy is a psychological topic suffering from historical neglect—a neglect that is increasingly consequential in an era of social media connectedness, mass surveillance, and the permanence of our electronic footprint. Despite fundamental changes in the privacy landscape, social and personality psychology journals remain largely unrepresented in debates on the future of privacy. By contrast, in disciplines like computer science and media and communication studies, engaging directly with sociotechnical developments, interest in privacy has grown considerably. In our review of this interdisciplinary literature, we suggest four domains of interest to psychologists. These are as follows: sensitivity to individual differences in privacy disposition, a claim that privacy is fundamentally based in social interactions, a claim that privacy is inherently contextual, and a suggestion that privacy is as much about psychological groups as it is about individuals. Moreover, we propose a framework to enable progression to more integrative models of the psychology of privacy in the digital age and in particular suggest that a group and social relations–based approach to privacy is needed.

Recent developments in political, technological, and social domains are leading to a direct challenge to our ability to exercise privacy. The privacy and security expert Bruce Schneier claims that surveillance is now the business model of the Internet (2015). Rather than being the customers of large digital technology companies, we are the product (Rushkoff, 2011; Schneier, 2015). Facebook founder Mark Zuckerberg (2010) has famously argued that the need for privacy is over and that withholding information could be seen as a selfish act. In the political sphere, privacy has moved centre stage after the revelations from Edward Snowden about the dragnet surveillance carried out by the

US (and allied) governments (beginning with Greenwald, 2013). From the technical perspective, the miniaturisation, mobilisation, and always-connected nature of new (artificially intelligent) Internet technologies (the 'Internet of Things', Ashton, 2009) mean that domains previously unreachable are now accessible: everything we do, everything we say, and everywhere we go can be known by others.

Given the key role that privacy plays in the development of normal psychological functioning, stable interpersonal relationships, and personal development (Altman, Vinsel, & Brown, 1981; Margulis, 2003b), you might expect that it would be a key feature of interest for psychologists. However, psychology has historically paid little attention to privacy (or technology, Kende, Ujhelyi, Joinson, & Greitemeyer, 2015; Margulis, 2003a; Wilson, Gosling, & Graham, 2012). This paper reviews the literature on privacy from computer science and media and communication studies, who have engaged with recent developments in digital technologies, and makes the case for how privacy concepts fit into classic domains of interest to social and personality psychologists. However, we go further than outlining separate psychological domains (e.g., personality vs. social psychology) and also set out a framework that will enable psychologists to develop integrative theories of the psychology of privacy that enrich the study of personal relationships, social interaction, and intra- and intergroup processes (see Augoustinos, Walker, & Donaghue, 2006, for a discussion of integrating social psychological theory). Integration may enable the resolution of various inconsistencies and duplicated efforts that have delayed privacy research thus far.

1 | DEFINING PRIVACY

Privacy is recognised by the United Nations as a universal human right, yet it has been described as an elastic (Allen, 1988; Margulis, 2003b) and evasive (Solove, 2002) concept. Traditional definitions of privacy (e.g., Warren & Brandeis, 1890) assume an individualistic "right to be let alone". However, for a psychological and interactional process-based approach to privacy, a useful definition can be found in Margulis (1977), where privacy is described as "selective control over transactions between self (or one's group) and others, the ultimate aim of which is to enhance autonomy and/or to minimise vulnerability" (p. 10). People need control over their transactions with others (to varying degrees) to experience the well-being that is associated with intimacy and emotional release (Westin, 1967). Moreover, privacy is needed for the protection of freedom of speech, freedom of association (Bloustein, 1976), and freedom from inequality and domination (Anthony, Campos-Castillo, & Horne, 2017; Hoye & Monaghan, 2018). Others have argued that privacy is not based on control, but more specifically that privacy is only achieved when one has limited access to themselves (Dienlin, 2019).

Several ways of classifying the dimensions of privacy exist in the literature. The most heavily researched is personal information privacy (Burgoon et al., 1989; DeCew, 1997). Other domains include interactional privacy , regarding quantity and quality of interactions with others (Burgoon et al., 1989; Laufer & Wolfe, 1977); territorial or physical privacy, regarding space, crowding, and being touched by others (Goffman, 1972; Klopfer & Rubenstein, 1977; Pastalan, 1970); psychological privacy, regarding our thoughts and feelings and the revelation of them (Burgoon et al., 1989); and expressive privacy, concerning expression of self or identity (DeCew, 1997; see similar ideas in Laufer & Wolfe, 1977). The degree to which these overlap has been discussed elsewhere (e.g. Joinson & Paine, 2007). The framework outlined in this paper is intended to be adaptable for all dimensions of privacy, but most of the literature to date relates to information privacy.

Self-disclosure is a closely related topic and unlike privacy has a longer tradition of being studied in psychology, particularly in clinical research. Disclosure research typically studies what people reveal about themselves, in what contexts, or how disclosure is done (see Berg & Derluga, 1987; Cozby, 1973; Dindia, Fitzpatrick, & Kenny, 1997; Joinson & Paine, 2007; Omarzu, 2000; Won-Doornink, 1985). For various reasons, including psychologists' lack of familiarity with privacy concepts (see Masur, 2018, for an extended discussion of this issue), self-disclosure research has been divorced from the study of privacy despite their obvious interrelatedness and situatedness in interactions and self-presentations (Antaki, Barnes, & Leudar, 2005; Goffman, 1959; Joinson & Paine, 2007; Masur, 2018).

The separation of topics speaks to the broader problem of narrow or insufficient privacy theory (Dienlin & Trepte, 2015; Margulis, 1977; Preibusch, 2013; Smith, Dinev, & Xu, 2011). A key example is the so called "privacy paradox" whereby people ostensibly claim to care about their privacy but openly share information about themselves (Norberg & Horne, 2007; Spiekermann, Grossklags, & Berendt, 2001). However, the privacy paradox can be resolved in some contexts—for example, when distinguishing between different dimensions of privacy and incorporating the psychological theory of planned behaviour (Ajzen, 1991; Dienlin & Trepte, 2015) or when linking privacy to identity consequences rather than the mere presence of surveillance (Stuart & Levine, 2017).

2 | THE HISTORICAL STUDY OF PRIVACY IN PSYCHOLOGY

In a pair of papers decades apart, Margulis (1977, 2003b) writes plaintively about the lack of interest in privacy in psychology (as did Westin, 1967). In the first review, Margulis (1977) points out that despite some early works, privacy research never developed out of its infancy. He describes the research in these early years as privacy orientations rather than theories. More than 20 years later, he writes in a disappointed tone that "there continues to be relative indifference to privacy, as a theoretical or research interest, among psychologists in general" (Margulis, 2003b, p. 243; see also review by Newell, 1995). There are current psychologists who study privacy (e.g., Buchanan, Paine, Joinson, & Reips, 2007; Joinson & Paine, 2007; Livingstone, 2006; Marder, Joinson, & Shankar, 2012); however, they tend to publish outside of social and personality psychology, such as in information science and human–computer interaction journals. Although their work has made significant impact in applying psychology to other disciplines, it has had less of an impact on the social/personality psychology mainstream. Conversely, an interest in privacy has burgeoned in a range of computer and social science disciplines—it is to these we now turn.

3 | COMPUTER, MEDIA, AND COMMUNICATION SCIENCES ON PRIVACY

We aim to review the literature on privacy in computer, media, communication, and other social science disciplines in a way that will be relevant to psychologists, arguing that the interdisciplinary research on privacy can be read through four main psychological lenses: individual personality differences in privacy orientation, privacy as dialectical and interactional, privacy as context-dependent, and privacy as a group-based phenomenon. In conducting this review, our aim is not to provide an exhaustive review of the entire literature, but rather to illustrate how privacy is relevant to theorising these core domains of social and personality psychology (for more on applications or measurement of privacy see reviews such as Acquisti, Brandimarte, & Loewenstein, 2015; Masur, 2018; Preibusch, 2013; Smith et al., 2011).

3.1 | Individual differences in privacy dispositions.

The first claim is that there may be individual differences in privacy disposition or concern for privacy (CFP), which acts as a generalised predictor of privacy behaviour across domains and technologies (Smith, Milberg, & Burke, 1996). The CFP perspective traditionally centres on concern about how information is collected, improper access, and concerns about disparate data being combined (Smith et al., 2011). Another commonly used measure builds on Westin (1967)'s privacy concepts and is used to classify people into "privacy fundamentalists", "privacy pragmatists", and the "privacy unconcerned", by asking people about their views on their generalised ability to obtain privacy (e.g., do they feel that consumers have lost all control over their personal information; see review by Kumaraguru & Cranor, 2005). The majority of people are found to be pragmatists who adapt their behaviour when they see fit, with approximately a third of the general population in the fundamentalist and 10% in the unconcerned categories (see Joinson, Paine, Buchanan, & Reips, 2006; Kumaraguru & Cranor, 2005; Sheehan, 2002, but for a critique see Jensen, Potts & Jensen, 2005).

Concern for privacy has been linked to personality traits (e.g., Junglas, Johnson, & Spitzmüller, 2008; Korzaan & Boswell, 2008; Taddicken, 2014). For example, Junglas et al. (2008) draw on protection motivation theory (Rogers, 1975) to understand how individual's personality traits influence their appraisal of threats, in particular finding that agreeableness is linked to lower CFP.

The privacy calculus approach uses these attitudinal measures, and people's evaluations of the costs and benefits of sharing or withholding, to study privacy behaviour (Dinev & Hart, 2006; Smith et al., 2011).

3.2 | Privacy is dialectical and interactional.

A second claim in the privacy literature is that privacy is dialectical—involving a shifting boundary regulation process of opening and closing at the same time, in which a person can have too much or not enough privacy (Altman et al., 1981). Inherent in this, and similar approaches, is the study of privacy and self-disclosure (e.g., partial disclosure behaviour) in social interactions, between individuals and small groups (Altman, 1974; Altman et al., 1981; Antaki et al., 2005; Palen & Dourish, 2003; Petronio, 2002; B. Schwartz, 1968). Interactional privacy can also refer to the regulation and separation of gatherings of people in spaces, including physical or digital interactions (Goffman, 1963; Joinson, Houghton, Vasalou, & Marder, 2011; Schwartz & Halegoua, 2015).

Communication privacy management (CPM) theory was developed by communications scholars (Petronio, 2002, 2015, building on Altman et al., 1981; Altman, 1974) and epitomises the interactional and dialectical view of privacy by focussing on how people collectively manage private objects (information)—such as managing how far the boundary spreads (i.e., who co-owns the private object), how permeable the boundary is (how confidential), what linkages exist between private objects, and the strategies that people use to restore privacy when the coregulation expectations have been breached.

3.3 | Privacy is contextually dependent.

The theory of privacy as contextual integrity (Nissenbaum, 2004, 2011) is based on the assumption that people desire to contain information within the context in which it was 'intended' and that each context is governed by norms of information flow. The privacy breach scenario—context collapse—is what happens when these norms are not upheld to the expected level, in ways that have unwanted consequences (boyd, 2001; Davis & Jurgenson, 2014). Multiple copresent audiences make upholding contextual information flow norms difficult (see Acquisti & Gross, 2006; boyd, 2010; Marder et al., 2012). The contextual integrity theory of privacy has seen extensive influence—including formalised models of contextual integrity that map norms of transmission between networks (Barth, Datta, Mitchell, & Nissenbaum, 2006; Criado & Such, 2015) and the elicitation and analysis of privacy requirements for computer software (Thomas, Bandara, Price, & Nuseibeh, 2014).

3.4 | Privacy can be a group-based property.

The final claim has received the least research attention (Smith et al., 2011), whereby privacy is regarded as selective control over access to one's group (Altman, 1974; Bloustein, 1976; Margulis, 2003b). Groups are a different unit of analysis than contexts because the processes of selective access (over information, interactions, and the expression of self) can concern a group entity and/or individuals as group member representatives. Moreover, groups can persist across contexts—for example, people want selective control over how much they reveal about and allow interaction with their family group while in their workplaces. Some groups represent systematic and stable stratifications in societies, and thus, a group-based privacy analysis has important implications for understanding social inequalities—for example, the targeting of minority groups with surveillance (Anthony et al., 2017; Hargittai & Litt, 2013; Park, Campbell, & Kwak, 2012).

There are two main approaches to group privacy in development: The first draws on CMP theory (as mentioned above), and the second borrows from the social identity approach (Tajfel & Turner, 1979; Turner, Hogg, Oakes, Reicher, & Wetherell, 1987). This latter perspective on privacy has thus far focussed on how people determine if individuals are in-group members with the same privacy norms and how they cope with conflicts between social identities or groups with different privacy norms (e.g., Calikli et al., 2016; Lampinen, Tamminen, & Oulasvirta, 2009; Price et al., 2017).

4 | UNITING THE PSYCHOLOGICAL DOMAINS

The continued separation of psychological domains has arguably been problematic for the discipline of psychology at large (e.g.,leading to duplicated efforts and gaps in knowledge); therefore, we now give a few examples where researchers have made concerted efforts to draw different domains and levels of privacy together. The first is by James, Nottingham, Collignon, Warkentin, and Ziegelmayer (2016) (based on Laufer & Wolfe, 1977). They integrate individual differences and interactional privacy, arguing that people have an *interpersonal privacy identity* that reflects the control an individual feels they should have over their personal information and that disclosure in social interactions involves the expression of a *privacy self-concept*. However, the model has yet to develop a clear account of how the individual and interactional might respond to or differ across social contexts or different sets of inter-group relations.

In another integrative study, Child and Agyeman-Budu (2010), drawing on CPM theory, combine individual difference and group levels by examining individuals management of group privacy (including self-monitoring skills and concern for appropriateness)[1]. Also inspired by CPM, De Wolf, Willaert, and Pierson (2014) bring together both individual and group level privacy management strategies in a study finding that privacy turbulence (i.e., a privacy concerning event) caused by oneself increases people's use of individual privacy management strategies, but privacy turbulence caused by others does not correspond with an increase in group privacy management strategies. However, while CPM pays some respect to contextual variation (Child & Petronio, 2011), the psychological mechanisms that create contextual variation in privacy needs and behaviours have not yet been explored.

An approach that integrates across three domains of privacy (individual, interactional, and contextual) is the machine learning approach of Barth et al. (2006). Drawing on the assumptions of a contextual integrity approach to privacy, individual agents' information flow frequencies are used to learn the norms of sharing between agents. By tracking individual agents across multiple interactions, this *reveals* (or infers) privacy contexts. As an inference of context, however, it cannot explain why individuals are adopting these sharing patterns. That is, it does not reveal the meanings of contexts. In contrast, situational privacy and self-disclosure theory (Masur, 2018) (which notably also incorporates self-disclosure theory) casts a distinction between the sociological construct of *contexts* (as predetermined settings) and psychological *situations* (comprised of people's perceptions of the setting).

Further, the multi-layered privacy interaction framework (Aeschlimann et al., 2015), based on Bronfenbrenner's (1977) ecological model of human development, situates the individual as socially embedded in a concentric system—from micro-level individual interactions, exo-level organisations, meso-level society, and macro-level state/government layers. The layers interact with each other and with the individual, so that people's decision-making can be affected by the privacy policies and violations that are executed at each of these levels, sometimes without individuals' knowledge. For example, Facebook as an organisation (exo-level) makes decisions about what privacy options they offer to users, which affects individual decisions about what they share on the social network.

Finally, the scale developed by Buchanan et al. (2007) integrates multiple domains of privacy, including information accessibility, expressive privacy (i.e., about the self), and physical privacy (e.g., someone invading your space), thus extending beyond the dominant focus on information privacy that has pervaded privacy research.

5 | GAPS AND ABSENCES IN THE PRIVACY RESEARCH BASE

Despite these attempts at integration, there are a number of gaps and absences in existing approaches to privacy that would need to be addressed to resolve ostensible paradoxes and inconsistencies in the study of privacy. In the following subsections, we expand on two concerns: (a) working towards distinguishing the different types of contexts of privacy and (b) the need to engage with the dynamics of privacy as it shifts across different domains and levels of interaction.

5.1 | Contexts in the digitally integrated world.

This gap in the privacy literature comes from the way context is conceptualised and on how groups and contexts are distinguished. There is general agreement that context is key to privacy (e.g., Barkhuus, 2012; Marwick & boyd, 2011; Nissenbaum, 2004) but not about how context should be conceptualised. For instance, Nissenbaum (2015) defines context as a physical place, a technology system/platform, a business model, a sector or industry, or a social domain; Masur (2018) emphasises psychological situations rather than contexts; Davis and Jurgenson (2014) define context as encompassing the shared meaning associated with a space, the people in it, and the associated identity meanings; under the social identity approach, context refers to a situation composed of a set of intra- or intergroup cues that make salient one of an individual's (psychologically relevant) identities, meaning that a change in the cues constitutes a change in context, while other aspects of the place can remain the same (see Turner, Hogg, Oakes, Reicher, & Wetherell, 1987). As a result of the complexity of defining context, research that talks about context often ends up studying social networks (e.g., Barth et al., 2006), but other elements of context are likely to be important for understanding privacy.

Based on our reading of the literature on context in privacy research, we propose considering a tripartite layered approach to contexts that accounts for the cyberphysical environmental, social context, and technical infrastructure elements of context. *Cyberphysical contexts* refer to the built environment (i.e., the design of places or spaces, including digital). The design of an environment affords the flow of movement and shapes communicative and behavioural actions (see Evans, Pearce, Vitak, & Treem, 2017; Norman, 2013). Privacy under this dimension is at risk when information crosses between environments (Evans et al., 2017). *Social contexts* are the more typical understanding of context as referred to by social scientists—the groups and individuals who occupy a space and have an investment in it. Davis and Jurgenson (2014) give the example of a wedding where guests from different aspects of one's social network are managed by strategically seating them at different tables (see also Binder, Howes, & Sutcliffe, 2009). Privacy is informed by an understanding of the social or cultural norms of relational conduct, that is, privacy is at risk when I or my confidants reveal my secrets to people in a different social network. Finally, the *technical infrastructure context* is the noninteractive infrastructure and architecture of environments—such as information flows that are created through unconfigurable technology design, or the materials that spaces are designed with, that cannot be altered. For example, an implanted device that measures my heart rate and has a preconfigured information flow transmitting data to my physician (via Wi-Fi). To understand privacy risks in this dimension of context, researchers would need to map technological configurations so as to identify privacy threats people may be unaware that they face. Distinguishing these ways of conceptualising context should create greater specificity in what privacy behaviours are afforded by context. Later, we suggest a framework for incorporating contexts and the dynamics of privacy.

5.2 | The dynamics of change in levels of privacy evaluations.

The second gap in the privacy literature is the need for a psychological understanding of the dynamics of changes in privacy evaluations and behaviours. These evaluations and behaviours concern different *domains of privacy* (informational, physical, interactional, etc.; see Buchanan et al., 2007), at *different levels of abstraction*

(e.g., sometimes privacy concerns manifest at the interindividual level and sometimes at the group level), and at *different time periods* (e.g., is my privacy at risk now or later?) (see Davis & Jurgenson, 2014).

There is only a small amount of research investigating these transitions or dynamics. For instance, it is suggested that an individual's privacy risk calculations may be momentarily replaced by collective privacy norms, if group threat is made salient (Aeschlimann et al., 2015; Cichy & Salge, 2015), and that people's self-disclosure decisions are made difficult when social spheres/contexts overlap (Joinson et al., 2011). The multilayered privacy interaction framework (Aeschlimann et al., 2015) explains how decisions made at different levels of society could affect individuals. It is possible that while some levels of privacy may influence each other (e.g., individual vs. group), others may not be correlated (e.g., physical vs. information privacy). The interrelatedness (or lack of) of domains and dimensions of privacy require further investigation.

We suggest that one way to deal with both of these gaps—in the conceptualisation of contexts and on the dynamics of privacy—is to draw on theory on the role of social identity in decision-making and behaviour (Turner, 1991), as it offers a model of how the moment-by-moment dynamic interactions between context and cognition can be understood. It can be used to explore how the different aspects of privacy might impact on the self—and how these might change as contexts change. This notion of a more dynamic self at the heart of privacy was foregrounded by Altman et al. (1981) who proposed that momentary states determine how accessible the self currently is to others (see also James et al., 2016; Margulis, 1977). The social identity approach also explains cognitive shifts between interpersonal, intragroup, and intergroup levels of interaction.

6 | A FRAMEWORK APPROACH TO MODELLING PRIVACY

Given the complexity of privacy, we do not suggest that there is one all-encompassing theory that can account for all aspects of privacy. Instead, we suggest that researchers utilise a framework approach (see Figure 1) where they select the substantive dimensions that are relevant for their domain of application and apply (existing) social and personality psychological theory as applicable to those psychological domains. Being deliberate in these choices will assist in determining which levels and domains of privacy are being captured in the study of privacy and which ones are not.

We set out the below framework with all of the possible levels of analysis. Research on privacy can be decomposed across them, or the framework itself can be used to extract privacy relevant dimensions from other psychological topics of interest (e.g., if interested in intergroup conflict, researchers could draw more on group privacy research). In form, and following the format of this paper, the model laid out below also essentially represents a model of how psychology itself is typically comprised. The dimensions are as follows: (a) the characteristics of the individual; (b) privacy in context; (c) the individual-interpersonal-intergroup level of interaction; (d) the dimension(s) of privacy, including information, territorial, expressive, or psychological; and (e) the source of privacy threat/need for regulation.

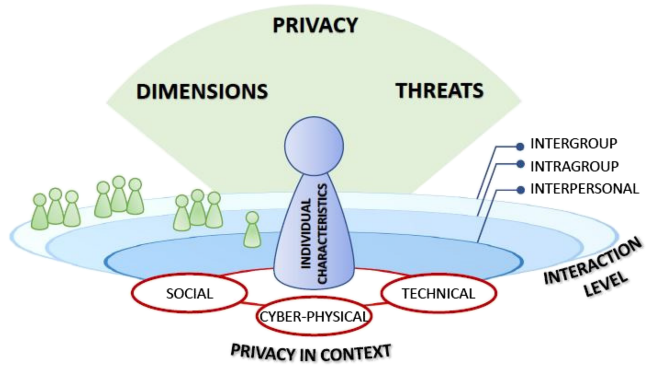

FIGURE 1 Visualisation of dynamic interlinked domains of a psychology of privacy framework

The *characteristics of the individual* begins with what an individual might bring to a privacy interaction—including personality dispositions, personal decision-making processes, and even neurological or physiological workings of privacy. The study of *privacy in context* can in turn be analysed across the cyberphysical environmental context, the social context, and the technical infrastructural context. Then, each *privacy-related interaction* can be analysed across three levels: privacy in interpersonal interactions, privacy in intragroup interactions, and privacy in intergroup interactions. Next, it is important to classify which *dimensions of privacy* are relevant to a privacy interaction—for example, whether it regards selective control over territories, information, physical privacy, the expression of identity, and so forth. Finally, the *source and nature of privacy threats* can occur at any level and from multiple locations. Privacy threats are traditionally thought of as arising from one of two sources: surveillance and exploitation by powerful entities or from listening in by our peers (Westin, 1967). Yet, there are also new forms of veillance that are less well understood, including sousveillance ('from below') (e.g., Mann, Nolan, & Wellman, 2002

The next step we envisage is to attempt integration of prominent approaches to privacy and their key insights. For instance, CPM theory (Petronio, 2002, 2010, 2015) and privacy as contextual integrity theory (Nissenbaum, 2004) are two theories that capture important insights into privacy, on regulating the co-ownership of private information, and people's expectations that information should stay within elected boundaries. However, they have never claimed to be complete theories of privacy (see Barth et al., 2006) and, furthermore, do not reference each other. Next, the multi-layered privacy interaction framework could help to situate individuals in the systems and organisations that they interact with and that influence their decision-making (Aeschlimann et al., 2015) and to furnish individuals with insights from social identity theory that could develop a dynamic interactional model of privacy. We also indicated placeholders for individual characteristics underpinning privacy evaluations and behaviour in the framework. An understanding of the extent to which these needs are stable versus malleable should feed into any dynamic account of privacy. These theories and approaches are not inherently incompatible, and integrations may lead to breakthroughs in understanding privacy behaviour; however, future research needs to evaluate the extent to which total theoretical integration is possible or desirable, which is why we suggested using a selective framework approach as a way of specifying which privacy dimensions and psychological domains are applicable to a problem area. We do not envisage the framework as a static description of the privacy space. How privacy shifts dynamically between these levels—and whether and how these levels might be in operation at one and the same time—are key theoretical and practical research questions.

7 | EXPANDING BEYOND PRIVACY

The outline of different privacy theories and approaches was the focus of this paper; however, there are several broader social issues that could incorporate privacy, and we briefly signpost towards these now. These subjects include the following: (a) *security*, the need for certainty, stability, and safety may compete or complement the need for privacy (Bansal, 2016; Dourish & Anderson, 2006; Solove, 2011), yet as far as we are aware, they have not been studied in unison and are rhetorically treated as a trade-off; (b) *surveillance studies* are an interdisciplinary effort that psychologists could contribute towards (Tucker, Ellis, & Harper, 2016). There is a research on personality traits and employer monitoring (Sayre & Dahling, 2016) and on the shared identities between surveillers and the surveilled (O'Donnell, Jetten, & Ryan, 2010a, 2010b; Stuart & Levine, 2017; Subašić, Reynolds, Turner, Veenstra, & Haslam, 2011); however, intergroup relations and resistance research in social psychology could further help situate the surveillance by studying which powerful groups are enacting their influence over less powerful groups, via surveillance, the vulnerabilities that some social groups face (Anthony et al., 2017; Park, 2013) and how this is allowed or resisted (see work on the elaborated social identity model in particular, Drury & Reicher, 2000; Reicher, 1996); (3) *risk taking*, *control*, and *trust* are further examples of concepts extensively studied in psychology and pertinent to privacy (notable studies combining the topics include Brandimarte, Acquisti, & Loewenstein, 2012; Joinson, Reips, Buchanan, & Paine Scholfield, 2010; Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014; Xu, Dinev, Smith, & Hart, 2011). Further

psychological theory that could help drive this area forward include protection motivation theory (Ardion, 2016; Rogers, 1975; Rogers & Prentice-Dunn, 1997), psychological reactance theory (Brehm, 1966), and motivational and identity approaches to decision-making (e.g., social identity theory; Tajfel & Turner, 1979). We suggest that these, and other topics, could feed into the privacy framework (see Figure 1) at any stage, but a fuller consideration of how exceeds the scope of this review.

8 | CONCLUSION

Privacy concerns selective control and withdrawal from transactions with others and others' transactions with us; sometimes, transactions are technologically mediated, but nonetheless, privacy is inherent to individual well-being and to understanding the dynamics of social relations (Altman, 1974; Anthony et al., 2017; Westin, 2003). The intention of this paper was to persuade social and personality psychologists to take a keener interest in this topic.

The review of the literature and framework we have suggested is intended as a guide towards filling in the gaps in existing privacy theory. We also suggested the theoretical approaches that we believe are the most suited to uncovering the psychological mechanisms and processes involved in privacy management in the digital age, in particular those theories that situate privacy in social and group relations, as increasingly digital technology captures more about the people and places that are associated with us (boyd, 2012; Koohikamali, Peak, & Prybutok, 2017; Petronio, 2002). It is essential to develop privacy theory in order to enable the engineering of privacy protection mechanisms into computer systems; to evaluate the privacy implications of new technological innovations; to develop computer systems that can use observable contextual phenomena, physical (e.g., location), physiological (e.g., heart rate), etc. to infer users' privacy needs; and to inform social policies and protections. Thus, the challenge we pose to psychologists is to use this framework to engage in the debate about the future of privacy. Through multidisciplinary work, we can have better theories and tools to undertake this research (Yarkoni, 2012). The study of privacy should not be an isolated, specialist field. Psychologists have the ability to develop a comprehensive theory of the psychology of privacy and have a professional and a moral responsibility to contribute to the debate over the changes in the privacy landscape. Without engaging, we may end up 'watching the very concept of privacy being rewritten under our noses' (to paraphrase Webb, 2015).

ACKNOWLEDGEMENTS

This work was supported by the Engineering and Physical Sciences Research Council grants: EP/K033433/1 (CeRes), Privacy Dynamics: Learning from the Wisdom of Groups, and EP/R013144/1, SAUSE: Secure, Adaptive, Usable Software Engineering.

ENDNOTE

[1] Self-monitoring skills relate to people' ability engage in situational regulation of their self-presentation (Snyder, 1974), and concern for appropriateness (Lennox & Wolfe, 1984) reflects people's attention to social comparison information and predicts peer pressure susceptibility.

ORCID

Avelie Stuart https://orcid.org/0000-0001-7711-6149
Arosha K. Bandara https://orcid.org/0000-0001-8974-0555
Mark Levine https://orcid.org/0000-0001-5696-6021

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347* (6221), 509–514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on Facebook. *PET*, 1–22.

Aeschlimann, L., Harasgama, R., Kehr, F., Lutz, C., Milanova, V., Müller, S., … Tamò-Larrieux, A. (2015). Re-setting the stage for privacy: A multi-layered privacy interaction framework and its application. *Mensch und Maschine-Symbiose oder Parasitismus*. Schriften der Assistierenden der Universität St. Gallen, Vol 9. Available at SSRN: https://ssrn.com/abstract=2559835

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society*. Totowa, NJ: Rowman & Littlefield.

Altman, I. (1974). Privacy: A conceptual analysis. In D. H. Carson (Ed.), *Man-environment interactions: Evaluations and applications*. Environmental Design Research Association: Washington, D.C.

Altman, I., Vinsel, A., & Brown, B. B. (1981). Dialectic conceptions in social psychology: An application to social penetration and privacy regulation. In *Advances in Experimental Social Psychology* (Vol. 14, pp. 107-160): New York: livAcademic Press, Inc.

Antaki, C., Barnes, R., & Leudar, I. (2005). Self-disclosure as a situated interactional practice. *British Journal of Social Psychology*, *44*(2), 181–199.

Anthony, D., Campos-Castillo, C., & Horne, C. (2017). Toward a sociology of privacy. *Annual Review of Sociology*, *43*(1), 249–269. https://doi.org/10.1146/annurev-soc-060116-053643

Ardion, B. (2016). Sealing one's online wall off from outsiders: Determinants of the use of Facebook's privacy settings among young Dutch users. *International Journal of Technology and Human Interaction (IJTHI)*, *12*(1), 21–34. https://doi.org/10.4018/IJTHI.2016010102

Ashton, K. (2009). That 'Internet of Things' thing. *RFID Journal*. Retrieved from. http://www.rfidjournal.com/articles/view?4986

Augoustinos, M., Walker, I., & Donaghue, N. (2006). *Social cognition: An integrated introduction* (2nd ed.). London: Sage Publications.

Bansal, G. (2016). Distinguishing between privacy and security concerns: An empirical examination and scale validation. *Journal of Computer Information Systems*, 1–14.

Barkhuus, L. (2012). The mismeasurement of privacy: Using contextual integrity to reconsider privacy in HCI. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Austin, Texas, USA.

Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. Paper presented at the Security and Privacy, 2006 IEEE Symposium.

Binder, J., Howes, A., & Sutcliffe, A. (2009, April). The problem of conflicting social spheres: effects of network structure on experienced tension in social network sites. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 965–974). ACM.

Bloustein, E. J. (1976). Group privacy: The right to huddle. *Rutgers-Cam LJ*, *8*, 219.

boyd, d (2001). Faceted id/entity: Managing representations in a digital world. In *Master of Science in Media Arts and Sciences*. Massachusetts: Massachusetts Institute of Technology.

boyd, d (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi (Ed.), *Networked self: Identity, community, and culture on social network sites* (pp. 39–58).

boyd, d (2012). Networked privacy. *Surveillance & Society*, *10*(3/4), 348–350.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2012). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. https://doi.org/10.1177/1948550612455931

Brehm, J. W. (1966). *A theory of psychological reactance*. New York: Academic Press.

Bronfenbrenner, U. (1977). Toward an experimental ecology of human development. *American psychologist*, *32*(7), 513.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157–165. https://doi.org/10.1002/asi.20459

Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships*, *6*, 131–158.

Calikli, G., Law, M., Bandara, A. K., Russo, A., Dickens, L., Price, B. A., … Nuseibeh, B. (2016, May). Privacy dynamics: Learning privacy norms for social software. In *Proceedings of the 11th International Symposium on Software Engineering for Adaptive and Self-Managing Systems* (pp. 47–56). ACM.

Child, J. T., & Agyeman-Budu, E. A. (2010). Blogging privacy management rule development: The impact of self-monitoring skills, concern for appropriateness, and blogging frequency. *Computers in Human Behavior*, *26*(5), 957–963. https://doi.org/10.1016/j.chb.2010.02.009

Child, J. T., & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet. In K. B. Wright & L. M. Webb (Eds.), *Computer-mediated communication in personal relationships* (pp. 21–40). New York: Peter Lang.

Cichy, P., & Salge, T. O. (2015). The evolution of privacy norms: Mapping 35 years of technology-related privacy discourse, 1980-2014. Paper presented at the 2015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015.

Criado, N., & Such, J. M. (2015). Implicit contextual integrity in online social networks. *Information Sciences*, *325*, 48–69. https://doi.org/10.1016/j.ins.2015.07.013

Davis, J. L., & Jurgenson, N. (2014). Context collapse: Theorizing context collusions and collisions. *Information, Communication & Society*, *17*(4), 476–485. https://doi.org/10.1080/1369118X.2014.888458

De Wolf, R., Willaert, K., & Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies on Facebook. *Computers in Human Behavior*, *35*, 444–454. https://doi.org/10.1016/j.chb.2014.03.010

DeCew, J. W. (1997). *In pursuit of privacy. Law, Ethics, and the Rise of Technology*. Ithaca: Cornell.

Dienlin, T. (2019). *What is privacy?* Retrieved from https://tobiasdienlin.com/2019/03/22/what-is-privacy/

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80.

Dourish, P., & Anderson, K. (2006). Collective information practice: emploring privacy and security as social and cultural phenomena. *Human-Computer Interaction*, *21*(3), 319–342.

Drury, J., & Reicher, S. (2000). Collective action and psychological change: The emergence of new social identities. *British Journal of Social Psychology*, *39*, 579–604. https://doi.org/10.1348/014466600164642

Evans, S. K., Pearce, K. E., Vitak, J., & Treem, J. W. (2017). Explicating affordances: A conceptual framework for understanding affordances in communication research. *Journal of Computer-Mediated Communication*, *22*(1), 35–52. https://doi.org/10.1111/jcc4.12180

Goffman, E. (1959). *The presentation of self in everyday life*. New York: Anchor Books.

Goffman, E. (1963). *Behaviour in public places: notes on the social order of gatherings*. New York: The Free Press.

Goffman, E. (1972). *Relations in public*. Harmondsworth: Penguin.

Greenwald, G. (2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved from www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order/

Hargittai, E., & Litt, E. (2013). New strategies for employment? internet skills and online privacy practices during people's job search. *IEEE security & privacy*, *11*(3), 38–45.

Hoye, J. M., & Monaghan, J. (2018). Surveillance, freedom and the republic. *European Journal of Political Theory*, *17*(3), 1–21.

James, T. L., Nottingham, Q., Collignon, S. E., Warkentin, M., & Ziegelmayer, J. L. (2016). The interpersonal privacy identity (IPI): development of a privacy as control model. *Information Technology Management*, *17*(4), 341–360. https://doi.org/10.1007/s10799-015-0246-0

Joinson, A. N., Houghton, D. J., Vasalou, A., & Marder, B. L. (2011). Digital crowding: Privacy, self-disclosure, and technology. In S. Trepte, & L. Reinecke (Eds.), *Privacy Online* (pp. 33–45). Berlin Heidelberg: Springer.

Joinson, A. N., Paine, C., Buchanan, T., & Reips, U.-D. (2006). Watching me, watching you: Privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom. *Journal of Information Science*, *32*(4), 334–343.

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the internet. In A. Joinson (Ed.), *Oxford handbook of internet psychology* (Vol. III) (pp. 237–252). Oxford: Oxford University Press.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Paine Scholfield, C. B. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, *25*(1), 1–24. https://doi.org/10.1080/07370020903586662

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems*, *17*(4), 387–402.

Kende, A., Ujhelyi, A., Joinson, A., & Greitemeyer, T. (2015). Putting the social (psychology) into social media. *European Journal of Social Psychology*, *45*(3), 277–278. https://doi.org/10.1002/ejsp.2097

Klopfer, P. H., & Rubenstein, D. I. (1977). The concept privacy and its biological basis. *Journal of Social Issues*, *33*(3), 52–65.

Koohikamali, M., Peak, D. A., & Prybutok, V. R. (2017). Beyond self-disclosure: Disclosure of information about others in social network sites. *Computers in Human Behavior*, *69*, 29–42. https://doi.org/10.1016/j.chb.2016.12.012

Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *The Journal of Computer Information Systems*, *48*(4), 15–24.

Kumaraguru, P., & Cranor, L. F. (2005). Privacy indexes: a survey of Westin's studies. Retrieved from repository.cmu.edu:

Lampinen, A., Tamminen, S., & Oulasvirta, A. (2009). "All my people right here, right now": Management of group co-presence on a social networking site.In *Proceedings of the ACM 2009 international conference on Supporting group work* (pp. 281–290). ACM.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42.

Lennox, R. B. & Wolfe, R. N. (1984). Revision of the Self-Monitoring Scale. *Journal of Personality and Social Psychology*, *6*, 1349–1364.

Livingstone, S. (2006). Children's privacy online: Experimenting with boundaries within and beyond the family. In R. Kraut, M. Brynin, & S. Kiesler (Eds.), *Computers, phones, and the internet: Domesticating information technology. Human technology interaction series* (pp. 145–167). New York, USA: Oxford University Press.

Mann, S., Nolan, J., & Wellman, B. (2002). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society*, *1*(3), 331–355.

Marder, B., Joinson, A., & Shankar, A. (2012). Every post you make, every pic you take, I'll be watching you: Behind social spheres on Facebook. Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on. IEEE, Hawaii.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, *33*(3), 5–21.

Margulis, S. T. (2003a). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, *59*(2), 411–429. https://doi.org/10.1111/1540-4560.00071

Margulis, S. T. (2003b). Privacy as a social issue and behavioral concept. *Journal of Social Issues*, *59*(2), 243–261.

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*, 114–133. https://doi.org/10.1177/1461444810365313

Masur, P. K. (2018). *Situational Privacy and Self Disclosure*. Springer.

Newell, P. B. (1995). Perspectives on privacy. *Journal of Environmental Psychology*, *15*(2), 87–104. https://doi.org/10.1016/0272-4944(95)90018-7

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48.

Norberg, P. A., & Horne, D. R. (2007). Privacy attitudes and privacy-related behavior. *Psychology and Marketing*, *24*(10), 829–847. https://doi.org/10.1002/mar.20186

Norman, D. (2013). *The design of everyday things: Revised and expanded edition: Basic Books (AZ)*.

O'Donnell, A. T., Jetten, J., & Ryan, M. K. (2010a). Watching over your own: How surveillance moderates the impact of shared identity on perceptions of leaders and follower behaviour. *European Journal of Social Psychology*, *40*, 1046–1061. https://doi.org/10.1002/ejsp.701

O'Donnell, A. T., Jetten, J., & Ryan, M. K. (2010b). Who is watching over you? The role of shared identity in perceptions of surveillance. *European Journal of Social Psychology*, *40*(1), 135–147. https://doi.org/10.1002/ejsp.615

Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Ft. Lauderdale, Florida, USA.

Park, Y. J. (2013). Offline status, online status: Reproduction of social categories in personal information skill and knowledge. *Social Science Computer Review*, *31*(6), 680–702.

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, *28*(3), 1019–1027.

Pastalan, L. A. (1970). Privacy as an expression of human territoriality. In *Spatial behavior of older people* (pp. 88–101). Michigan: University of Michigan Press.

Petronio, S. (2002). *Boundaries of privacy: Dialetics of disclosure*. USA: State University of New York Press.

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory and Review*, *2*, 175–196. https://doi.org/10.1111/j.1756-2589.2010.00052.x

Petronio, S. (2015). Communication privacy management theory. In *The International Encyclopedia of Interpersonal Communication*. John Wiley & Sons, Inc.

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *Int. J.Human-ComputerStudies*, *71*, 1133–1143.

Price, B. A., Stuart, A., Calikli, G., Mccormick, C., Mehta, V., Hutton, L., … Nuseibeh, B. (2017). Logging you, Logging me: A replicable study of privacy and sharing behaviour in groups of visual lifeloggers. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *1*(2), 22.

Reicher, S. (1996). The battle of Westminster': Developing the social identity model of crowd behaviour in order to explain the initiation and development of collective conflict. *European Journal of Social Psychology*, *26*, 115–134. https://doi.org/10.1002/(SICI)1099-0992(199601)

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The journal of psychology*, *91*(1), 93–114.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of health behavior research 1: Personal and social determinants* (pp. 113–132). New York, NY: US, Plenum Press.

Rushkoff, D. (Producer). (2011). *You are Facebook's product, not customer*. WIRED. https://www.wired.co.uk/article/doug-rushkoff-hello-etsy

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior. *The Journal of Social Psychology*, *154*(4). https://doi.org/10.1080/00224545.2014.914881

Sayre, G. M., & Dahling, J. J. (2016). Surveillance 2.0: How personality qualifies reactions to social media monitoring policies. *Personality and Individual Differences*, *90*, 254–259. https://doi.org/10.1016/j.paid.2015.11.021

Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world: W. W. Norton & Company.

Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology*, *73*(6), 741–752.

Schwartz, R., & Halegoua, G. R. (2015). The spatial self: Location-based identity performance on social media. *New Media & Society*, *17*(10), 1643–1660. https://doi.org/10.1177/1461444814531364

Sheehan, K. B. (2002). Toward a typology of internet users and online privacy concerns. *The Information Society*, *18*(1), 21–32. https://doi.org/10.1080/01972240252818207

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Q.*, *35*(4), 989–1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly*, *20*(2), 167–196. https://doi.org/10.2307/249477

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, *90*(4), 1087–1156.

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. New Haven, Connecticut: Yale University Press.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce* (pp. 38–47). ACM.

Stuart, A., & Levine, M. (2017). Beyond 'nothing to hide': When identity is key to privacy threat under surveillance. *European Journal of Social Psychology*, *47*(6), 694–707. https://doi.org/10.1002/ejsp.2270

Subašić, E., Reynolds, K. J., Turner, J. C., Veenstra, K. E., & Haslam, S. A. (2011). Leadership, power and the use of surveillance: Implications of shared social identity for leaders' capacity to influence. *The Leadership Quarterly*, *22*(1), 170–181. https://doi.org/10.1016/j.leaqua.2010.12.014

Snyder, M. (1974). Self-monitoring of expressive behavior. *Journal of Personality and Social Psychology*, *30*(4), 526–537.

Taddicken, M. (2014). The 'Privacy Paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. https://doi.org/10.1111/jcc4.12052

Tajfel, H., & Turner, J. C. (1979). An integrative theory of intergroup conflict. In S. Worchel, & W. G. Austin (Eds.), *The social psychology of intergroup relations* (pp. 33–47). Monterey, CA: Brooks/Cole.

Thomas, K., Bandara, A. K., Price, B. A., & Nuseibeh, B. (2014). Distilling privacy requirements for mobile applications. Paper presented at the 36th International Conference on Software Engineering (ICSE 2014), Hyderabad, India.

Tucker, I., Ellis, D., & Harper, D. (2016). Experiencing the 'surveillance society. *The Psychologist*, *29*, 682–685.

Turner, J. C. (1991). *Social influence*. Buckingham, UK: Open University Press.

Turner, J. C., Hogg, M. A., Oakes, P. J., Reicher, S. D., & Wetherell, M. S. (1987). *Rediscovering the social group: A self-categorization theory*. Oxford: Blackwell.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220. https://doi.org/10.2307/1321160

Webb, G. (2015). Say goodbye to privacy. WIRED. Retrieved March 31, 2016 from http://www.wired.com/insights/2015/02/say-goodbye-to-privacy/.

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431–453. https://doi.org/10.1111/1540-4560.00072

Wilson, R. E., Gosling, S. D., & Graham, L. T. (2012). A review of Facebook research in the social sciences. *Perspectives on Psychological Science*, *7*(3), 203–220.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798.

Yarkoni, T. (2012). Psychoinformatics new horizons at the interface of the psychological and computing sciences. *Current Directions in Psychological Science*, *21*(6), 391–397.

Zuckerberg, M. (2010). *Facebook CEO Mark Zuckerberg TechCrunch interview at the Crunchies/Interviewer: M. Arrington*. San Francisco: TechCrunch, Crunchie awards.

AUTHOR BIOGRAPHIES

Dr Avelie Stuart completed her Social Psychology PhD in 2014 at Murdoch University, Western Australia, and is now a postdoctoral research fellow in Psychology at the University of Exeter, working on interdisciplinary projects relating to the development of privacy-sensitive and usable digital technologies, and is interested in using technology to study social identities, social networks, privacy, surveillance, and healthcare management. She is also more generally interested in studying social groups and collective behaviour.

Arosha K. Bandara is Professor of Software Engineering at The Open University, whose research and teaching focusses on software engineering for adaptive systems. Arosha has a particular interest in techniques for building adaptive security and privacy mechanisms for ubiquitous, Internet of Things (IoT) systems, and has developed approaches for engineering adaptive mechanisms for network access control, cloud software services, as well as quantitative metrics for privacy risks in social networks. He is also interested in mechanisms for supporting engineers in designing and building privacy-aware systems, for example, developing a Privacy by Design framework for IoT applications (https://doi.org/10.1016/j.ins.2019.09.061). Arosha completed his PhD at Imperial College London, UK in 2005, prior to which he worked as a senior software engineer at Sapient Corporation, USA. He is the lead educator for the OU's successful "Introduction to Cyber Security" MOOC.

Mark Levine is a Professor of Social Psychology at Lancaster University and the University of Exeter. His research focuses on the role of social identities and group processes in prosocial and antisocial behaviour. He is particularly interested in the research possibilities afforded by new technologies and digital data. He has a well-established track record of interdisciplinary research with computer scientists and software engineers. This work has included systematic behavioural analysis of CCTV footage of real-life violent incidents; using natural language processing of online data to examine social identity processes; and the study of the psychological dimensions of both privacy and surveillance.

How to cite this article: Stuart A, Bandara AK, Levine M. The psychology of privacy in the digital age. *Soc Personal Psychol Compass*. 2019;e12507. https://doi.org/10.1111/spc3.12507